What is claimed is:

1. A debug system comprising:

a microprocessor operable to store secret program information; and

a host computer that is connected to the microprocessor so as to debug the program information in the microprocessor, wherein

the microprocessor includes:

a nonvolatile memory which (i) has an area for storing key information that is used to securely handle program information and (ii) is writable only once;

a writing unit operable to, if no key information is stored in the nonvolatile memory, receive key information from the host computer and write the key information into the nonvolatile memory; and

a first transmission unit operable to securely perform transmission of program information with the host computer using the key information that has been written into the nonvolatile memory,

the key information that has been written into the nonvolatile memory is not readable outside of the microprocessor, and

the host computer includes:

a receiving unit operable to receive key information from a user;

a sending unit operable to store therein the key information received from the user and send the key information to the microprocessor; and

a second transmission unit operable to securely perform transmission of program information with the microprocessor using the key information stored in the sending unit.

2. A microprocessor which is operable to store secret program information and is connected to a host computer that is used to debug the program information in the microprocessor, comprising:

a program information storing unit operable to store the program information which is one of a program, data and a program and data;

an executing unit operable to read the program information to perform an operation corresponding to the read program information;

a nonvolatile memory which (a) has an area for storing key information that is used to securely handle program information and (b) is writable only once;

a writing unit operable to, if no key information is stored in the nonvolatile memory, receive key information from the host computer and write the received key information into the nonvolatile memory; and

a transmission unit operable to securely perform transmission of program information with the host computer using the key information that has been written into the nonvolatile memory, wherein

the key information that has been written into the nonvolatile memory is not readable outside of the microprocessor.

3. The microprocessor of Claim 2, wherein

the nonvolatile memory additionally stores therein flag information that indicates whether key information is stored in the nonvolatile memory,

the transmission unit reads the flag information, and

if the read flag information indicates that no key information is stored in the nonvolatile memory, the writing unit receives the key information from the host computer, and writes the key information received from the host computer into the nonvolatile memory.

4. The microprocessor of Claim 3, wherein

the transmission unit includes:

an encryption unit operable to encrypt the program information stored in the program information storing unit using the key information that has been stored in the nonvolatile memory; and

an output unit operable to output the encrypted program

information.

5. The microprocessor of Claim 4, wherein

the transmission unit further includes

an inhibition unit operable to, in response to a request from the host computer, inhibit the output unit from outputting the encrypted program information.

6. The microprocessor of Claim 4, wherein

the transmission unit further includes:

an inhibition condition storing unit storing an inhibition condition that relates to the key information received from the host computer; and

an inhibition unit operable to, if the key information received from the host computer satisfies the inhibition condition, inhibit the output unit from outputting the encrypted program information.

7. The microprocessor of Claim 3, wherein

the program information stored in the program information storing unit is encrypted program information which is one of an encrypted program, encrypted data, and an encrypted program and encrypted data,

the executing unit (i) reads the key information that has been stored in the nonvolatile memory, (ii) decrypts the

encrypted program information using the read key information so as to generate decrypted program information which is one of a decrypted program, decrypted data, and a decrypted program and decrypted data, and (iii) performs an operation corresponding to the decrypted program information, wherein

the transmission performed by the transmission unit is transmission of encrypted program information.

8. The microprocessor of Claim 5, wherein

the executing unit encrypts a result of the operation using the key information that has been stored in the nonvolatile memory, and writes the encrypted result into the program information storing unit.

9. The microprocessor of Claim 5,wherein

the program stored in the program information storing unit is an encrypted program, and

the program information storing unit has a path to communicate with an external device.

10. The microprocessor of Claim 5, wherein

the key information that has been written into the nonvolatile memory is constituted by one or more pieces of partial key information,

the program stored in the program information storing unit

is a plurality of encrypted partial programs each of which corresponds to any of the pieces of partial key information, and

the executing unit (a) reads a piece of partial key information from the nonvolatile memory, (b) reads one or more of the encrypted partial programs corresponding to the read piece of partial key information, from the program information storing unit, (c) decrypts the read encrypted partial programs using the read piece of partial key information to generate decrypted partial programs, and (d) performs an operation corresponding to the decrypted partial programs.

11. The microprocessor of Claim 3, further including a cache memory, wherein

the program information stored in the program information storing unit is encrypted program information which is one of an encrypted program, encrypted data, and an encrypted program and encrypted data,

the executing unit (a) reads the key information that has been stored in the nonvolatile memory, (b) decrypts the encrypted program information using the read key information so as to generate decrypted program information which is one of a decrypted program, decrypted data and a decrypted program and decrypted data, (c) writes the decrypted program information into the cache memory, (d) reads the decrypted program

information from the cache memory in accordance with a processing speed of the executing unit, and (e) performs an operation corresponding to the decrypted program information, and

the transmission performed by the transmission unit is transmission of encrypted program information.

12. The microprocessor of Claim 2, wherein

the nonvolatile memory additionally stores flag information indicating whether the key information is stored in the nonvolatile memory,

the transmission unit reads the flag information,

if the read flag information indicates that no key information is stored in the nonvolatile memory, the transmission unit reads the program information from the program information storing unit and outputs the read program information to the host computer, and

if the read flag information indicates that the key information has been stored the nonvolatile memory, the transmission unit reads the program information from the program information storing unit, encrypts the read program information using the key information that has been stored in the nonvolatile memory, and outputs the encrypted program information to the host computer.

13. A host computer which (i) is connected to a

microprocessor operable to store secret program information and (ii) debugs the program information in the microprocessor, comprising:

a receiving unit operable to receive key information from a user;

a sending unit operable to store the received key information therein and send the received key information to the microprocessor; and

a transmission unit operable to securely perform transmission of program information with the microprocessor using the key information stored in the sending unit.

14. The host computer of Claim 13, wherein

the transmission unit includes:

a program information receiving unit operable to receive, from the microprocessor, encrypted program information which has been generated by encrypting the program information;

a decrypting unit operable to decrypt the encrypted program information using the key information stored in the sending unit so as to generate decrypted program information; and

a display unit operable to display the decrypted program information generated by the decrypting unit.

15. The host computer of Claim 14, wherein

the transmission unit further includes:

a program information input unit operable to receive, from the user, program information which is one of a program, data and a program and data;

an encrypting unit operable to encrypt the program information received from the user, using the key information stored in the sending unit so as to generate encrypted program information; and

an output unit operable to output the encrypted program information generated by the encrypting unit to the microprocessor.

16. The host computer of Claim 14, further comprising:

a storage unit storing a source program;

a conversion unit operable to convert the source program into an object program; and

an encrypting unit operable to encrypt the object program using the key information stored in the sending unit so as to generate an encrypted program, wherein

the transmission unit transmits the encrypted program generated by the encrypting unit to the microprocessor.

17. The host computer of Claim 14, wherein

the transmission unit further includes:

an inhibition condition storing unit storing an inhibition condition that relates to the key information; and

an inhibition request output unit operable to, if the key information satisfies the inhibition condition, output a request, to the microprocessor, to inhibit the transmission of the encrypted program information.

18. A read/write device that is connected to a microprocessor operable to store secret program information, comprising:

a receiving unit operable to receive key information from a user;

a sending unit operable to store the received key information therein and send the received key information to the microprocessor; and

a transmission unit operable to securely perform transmission of program information with the microprocessor using the key information.